

Congruences for Jacobi Sums

Ronald Evans

*Department of Mathematics, 0112, University of California at San Diego,
La Jolla, California 92093-0112
E-mail: revans@ucsd.edu*

Communicated by Y. Ihara

Received August 5, 1997

A congruence for Jacobi sums of order k over finite fields is proved, which generalizes a congruence of Iwasawa (1975) for prime k and Ihara (1986) for prime power k .

[View metadata, citation and similar papers at core.ac.uk](#)

1. INTRODUCTION

Let χ denote a multiplicative character of order $k > 2$ on a finite field F_q , and write $q = kf + 1$. In this paper, we will obtain congruences for the Jacobi sums

$$J(a, b) = - \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} \chi^a(\alpha) \chi^b(-1 - \alpha), \quad (1.1)$$

where a and b are integers (mod k). Note that the sum $\sum_{\alpha \neq 0, -1} \chi^a(\alpha) \chi^b(1 - \alpha)$, also called a Jacobi sum, differs from that in (1.1) by a factor of $-\chi^c(-1)$, where

$$c = -a - b. \quad (1.2)$$

By replacing α by $-1 - \alpha$ and by α^{-1} in (1.1), we see that

$$J(a, b) = J(b, a) = J(c, b) = J(b, c) = J(c, a) = J(a, c). \quad (1.3)$$

If a , b , or c is divisible by k , then the Jacobi sum $J(a, b)$ is easily evaluated, viz., $J(0, 0) = 2 - q$, and $J(0, b) = \chi^b(-1)$, where $k \nmid b$. From now on, assume that

$$k \nmid a, \quad k \nmid b, \quad \text{and} \quad k \nmid c. \quad (1.4)$$

Write

$$\zeta = e^{2\pi i/k}, \quad \lambda = 1 - \zeta, \quad \lambda_a = 1 - \zeta^a. \quad (1.5)$$

One object of this paper is to give an elementary proof of Theorem 1 below, in which we evaluate $J(a, b)$ modulo $(1 - \zeta^a)(1 - \zeta^b)(1 - \zeta^c)$. By dividing each of a, b, k by $\gcd(a, b, k)$, if necessary, we may assume that $\gcd(a, b, k) = 1$, that is, $J(a, b)$ has order k .

THEOREM 1. *Let $k > 2$ be an integer. Given integers a, b, c with $c = -a - b$, $k \nmid a, k \nmid b, k \nmid c$, and $\gcd(a, b, k) = 1$, we have, modulo $(1 - \zeta^a)(1 - \zeta^b)(1 - \zeta^c)$,*

$$J(a, b) \equiv \begin{cases} 2 - q, & \text{if } k = 3, \\ 1 + i(q - 1)/2, & \text{if } k = 4, \\ \chi(-1), & \text{if } k > 4. \end{cases} \quad (1.6)$$

Note that $\chi(-1) = 1$ if q is even, and $\chi(-1) = (-1)^f$ if q is odd.

Theorem 1 was proved for prime k by Iwasawa [7] in 1975 and (by different methods) for prime power k by Ihara [6, p. 81] in 1986. The proofs of Iwasawa and Ihara both rely on deep algebraic methods. In contrast, our proof is elementary and self-contained.

Miki [8, Theorem 2] has given a congruence (for multiple Jacobi sums with two or more arguments) which greatly extends the special case of Theorem 1 in which k is a power of a prime l with $\gcd(abc, l) = 1$, when $l > 3$. (Miki's congruence for $l = 2$ is weaker than this special case of Theorem 1.) A version of this case of Theorem 1 for multiple Jacobi sums may be found in the book of Gouvêa and Yui [5, Proposition 1.7]. For a simple application of Theorem 1 in the case $k = 4$, see Abo, Sasakura, and Terasoma [1, p. 284].

The proof of Theorem 1 is given in Section 3. It depends on an interesting result (Proposition 5) on cyclotomic numbers of order k , proved in Section 2. Section 2 also contains some related propositions which will be used to prove subsequent theorems.

In the case where $k \geq 8$ is a power of 2, we extend Theorem 1 as follows.

THEOREM 2. *Let $k > 8$ be a power of 2 and choose integers a, b, c with $c = -a - b$, $k \nmid a, k \nmid b, k \nmid c$, and $\gcd(a, b, k) = 1$, with, say, b even. Then we have, modulo $(1 - \zeta^a)(1 - \zeta^b)(1 - \zeta^c)(1 - \zeta)$,*

$$J(a, b) \equiv \begin{cases} \chi(-1) + (1 - \zeta^a)(1 - \zeta^b)(1 - \zeta)kf/8, & \text{if } 2 \text{ is a 4th power in } F_q^*, \\ \chi(-1) + (1 - \zeta^a)(1 - \zeta^b)(1 - \zeta)(1 + kf/8), & \text{otherwise.} \end{cases} \quad (1.7)$$

We remark that 2 is always a square in F_q^* in the context of Theorem 2; for if $q = p^r$ with p an odd prime, then either $p \equiv 1 \pmod{8}$ or $2 \mid r$.

An elementary proof of Theorem 2 is given in Section 4, with the aid of Proposition 8. A special case of Theorem 2 was proved by Evans [4, Eq. (26)].

In Section 5, we use Proposition 7 to give an elementary proof of the following result.

THEOREM 3. *Let $k > 4$ be even. Suppose that a and b are odd, d is even, and neither d nor $b - a$ is divisible by k . Then we have, modulo $(1 - \zeta^d)(1 - \zeta^{b-a})(1 - \zeta^2)$,*

$$J(a, d) \equiv J(b, d). \quad (1.8)$$

In particular, the congruence (1.8) holds modulo $(1 - \zeta^2)^3$.

It will be seen in (5.2) that when $k = 4$,

$$J(1, 2) \equiv J(3, 2) + 4if \pmod{8}. \quad (1.9)$$

This shows that Theorem 3 does not hold when $k = 4$ and f is odd.

In Section 6, we apply Theorem 1 to prove the following corollary of Theorem 3.

COROLLARY 4. *Let $k > 2$ be twice an odd prime power. Let a be odd and d even, with $k \nmid d$. Then*

$$J(a, d) \equiv \begin{cases} \chi(-4^d) \pmod{(1 - \zeta^2)^3}, & \text{if } k \nmid 3d, \\ (2 - q) \chi(-4^d) \pmod{(1 - \zeta^2)^3}, & \text{if } k \mid 3d. \end{cases} \quad (1.10)$$

Corollary 4 generalizes a result of Acharya and Katre [2, p. 59], wherein $k/2$ is an odd prime and the modulus is $(1 - \zeta^2)^2$.

2. CONGRUENCES FOR SUMS OF CYCLOTOMIC NUMBERS

Fix a generator γ of F_q^* such that $\chi(\gamma) = \zeta$. For $\alpha \in F_q^*$, define $\text{ind}(\alpha)$ to be the integer $u \pmod{q-1}$ for which $\alpha = \gamma^u$. For integers $s, t \pmod{k}$, the cyclotomic number $(s, t)_k$ is defined to be the number of $\alpha \in F_q - \{0, -1\}$ for which both $\chi(\alpha) = \zeta^s$ (i.e., $\text{ind}(\alpha) \equiv s \pmod{k}$) and $\chi(1 + \alpha) = \zeta^t$ (i.e., $\text{ind}(1 + \alpha) \equiv t \pmod{k}$). By replacing α by α^{-1} , it is easily seen that

$$(s, t)_k = (-s, t - s)_k. \quad (2.1)$$

Observe that $\sum_{t=0}^{k-1} (s, t)_k$ counts the number of $\alpha \in F_q - \{0, -1\}$ for which $\chi(\alpha) = \zeta^s$. This is the number of integers i with $0 \leq i \leq f-1$ such that $\gamma^{s+ik} \neq -1$. Thus, for $0 < s < k$,

$$\sum_{t=0}^{k-1} (s, t)_k = f - \varepsilon(s, k, f), \quad (2.2)$$

where

$$\varepsilon(s, k, f) = \begin{cases} 1, & \text{if } s = k/2, 2 \mid k, \text{ and } 2 \nmid f \\ 0, & \text{otherwise.} \end{cases} \quad (2.3)$$

We are now prepared to prove congruences for certain sums of cyclotomic numbers

PROPOSITION 5. *Define*

$$L := \sum_{s, t=0}^{k-1} st(s, t)_k. \quad (2.4)$$

If k is odd, then

$$L \equiv \begin{cases} 0 \pmod{k}, & \text{if } 3 \nmid k, \\ fk/3 \pmod{k}, & \text{if } 3 \mid k. \end{cases} \quad (2.5)$$

If k is even, then

$$L \equiv \begin{cases} fk/4 \pmod{k/2}, & \text{if } 3 \nmid k \text{ and } 4 \mid k, \\ 0 \pmod{k/2}, & \text{if } 3 \nmid k \text{ and } 2 \parallel k, \\ fk/12 \pmod{k/2}, & \text{if } 3 \mid k \text{ and } 4 \mid k, \\ -fk/6 \pmod{k/2}, & \text{if } 3 \mid k \text{ and } 2 \parallel k. \end{cases} \quad (2.6)$$

Proof. Replacing s by $-s$ and t by $t-s$ in (2.4), we obtain

$$L \equiv \sum_{s, t \pmod{k}} (s^2 - st)(s, t)_k \pmod{k}, \quad (2.7)$$

by (2.1). Thus

$$2L \equiv \sum_{s=1}^{k-1} s^2 \sum_{t=0}^{k-1} (s, t)_k \pmod{k}. \quad (2.8)$$

By (2.2) and (2.8),

$$2L \equiv f(k-1)(2k-1)k/6 - \varepsilon(k/2, k, f)k^2/4 \pmod{k}. \quad (2.9)$$

If k is odd, then multiplication of (2.9) by $(k+1)/2$ yields

$$L \equiv f(k^2-1)(2k-1)k/12 \pmod{k},$$

which in turn yields (2.5).

If k and f are both even, then by (2.9),

$$L \equiv f(k-1)(2k-l)(k/2)/6 \pmod{k/2},$$

which yields (2.6) in this case.

Finally, if k is even and f is odd, then by (2.9),

$$L \equiv (f(k-1)(2k-1) - 3(k/2))k/12 \pmod{k/2},$$

which yields the remaining case of (2.6). ■

The following corollary of Proposition 5 is immediate.

COROLLARY 6. *If k is a power of a prime y , then*

$$L \equiv \begin{cases} f \pmod{3}, & \text{if } k=3, \\ f \pmod{2}, & \text{if } k=4, \\ 0 \pmod{k}, & \text{if } k>4, y>3, \\ 0 \pmod{k/4}, & \text{if } k>4, y=2, \\ 0 \pmod{k/3}, & \text{if } k>4, y=3. \end{cases} \quad (2.10)$$

PROPOSITION 7. *Let k be even, and define*

$$N := \sum_{\substack{s, t=0 \\ s \text{ even}}}^{k-1} st(s, t)_k, \quad M := \sum_{s, t=0}^{k-1} (-1)^s st(s, t)_k. \quad (2.11)$$

Then

$$N \equiv \begin{cases} fk/6 \pmod{k/2}, & \text{if } 3|k, \\ 0 \pmod{k/2}, & \text{if } 3 \nmid k, \end{cases} \quad (2.12)$$

and

$$M \equiv \begin{cases} fk/4 \pmod{k/2}, & \text{if } 4 \mid k, \\ 0 \pmod{k/2}, & \text{if } 2 \parallel k. \end{cases} \quad (2.13)$$

Proof. Just as in the proof of (2.8),

$$2N \equiv \sum_{\substack{s \pmod{k} \\ s \text{ even}}} s^2 \sum_{t \pmod{k}} (s, t)_k \pmod{k}. \quad (2.14)$$

By (2.2) and (2.14),

$$N \equiv \frac{1}{2} f \sum_{\substack{s \pmod{k} \\ s \text{ even}}} s^2 \equiv fk(k-1)(k-2)/12 \pmod{k/2},$$

and (2.12) easily follows. Finally, since $M = 2N - L$, (2.13) follows from (2.12) and (2.6). ■

PROPOSITION 8. *Let k be even. If s is an integer not divisible by k , then*

$$\text{ind}(1 - \gamma^{fs}) \equiv \sum_{t=1}^{k-1} t(s + fk/2, t)_k \pmod{k} \quad (2.15)$$

and

$$\text{ind}(2) \equiv \begin{cases} \sum_{\substack{s, t \pmod{k} \\ s \text{ odd}}} t(s, t)_k \pmod{k}, & \text{if } 4 \mid fk, \\ \sum_{\substack{s, t \pmod{k} \\ s \text{ even}}} t(s, t)_k \pmod{k}, & \text{if } 2 \parallel fk. \end{cases} \quad (2.16)$$

Proof. Over F_q ,

$$1 - x^f = \prod_{i=0}^{f-1} (1 - x\gamma^{ik}).$$

Thus, if $k \nmid s$,

$$\text{ind}(1 - \gamma^{fs}) \equiv \sum_{i=0}^{f-1} \text{ind}(1 + \gamma^{s+fk/2+ik}) \pmod{q-1},$$

and so

$$\begin{aligned} \text{ind}(1 - \gamma^{fs}) &\equiv \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1 \\ \text{ind}(\alpha) \equiv s + fk/2 \pmod{k}}} \text{ind}(1 + \alpha) \\ &\equiv \sum_{t \pmod{k}} t(s + fk/2, t)_k \pmod{k}, \end{aligned}$$

which proves (2.15).

Over F_q , since k is even,

$$x^{k/2} + 1 = \prod_{\substack{s=1 \\ s \text{ odd}}}^{k-1} (x - \gamma^{fs}).$$

Putting $x = 1$, we obtain

$$\text{ind}(2) \equiv \sum_{\substack{s \pmod{k} \\ s \text{ odd}}} \text{ind}(1 - \gamma^{fs}) \pmod{q-1}.$$

In view of (2.15), this proves (2.16). ■

3. PROOF OF THEOREM 1

By replacing $J(a, b)$ by an algebraic conjugate in $\mathbb{Q}(\zeta)$, we may assume without loss of generality that

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1. \quad (3.1)$$

Now,

$$J(a, b) = F + E, \quad (3.2)$$

where

$$F := - \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} (1 - \chi^a(\alpha))(1 - \chi^b(-1 - \alpha)) \quad (3.3)$$

and

$$E := q - 2 + \chi^a(-1) + \chi^b(-1). \quad (3.4)$$

Note that every summand in (3.3) is divisible by $(1 - \zeta^a)(1 - \zeta^b) = \lambda_a \lambda_b$.

Assume first that the root of unity ζ^c fails to have prime power order (so that in particular, k is not a prime power). Then $1 - \zeta^c$ is a unit, and it suffices to prove the congruence (1.6) modulo $\lambda_a \lambda_b$. By (3.2), it suffices to show that

$$E \equiv \chi(-1) \pmod{\lambda_a \lambda_b}. \quad (3.5)$$

By (3.4),

$$E \equiv \chi^a(-1) + \chi^b(-1) - 1 \pmod{\lambda_a \lambda_b},$$

since $\lambda_a \lambda_b$ divides k . If $\chi(-1) = 1$, then (3.5) follows. If $\chi(-1) = -1$ (so that $2 \mid k$), then (3.5) again follows if a and b have opposite parity. If $\chi(-1) = -1$ with a and b both odd, then (at least) one of $1 - \zeta^a$, $1 - \zeta^b$ is a unit and the other divides 2, so that (3.5) again follows. This completes the proof of Theorem 1 when ζ^c does not have prime power order. By symmetry, the proof is complete if any of $\zeta^a, \zeta^b, \zeta^c$ fails to have prime power order. Thus assume that ζ^a, ζ^b , and ζ^c each have prime power order.

If k is divisible by a product of two coprime prime powers > 1 , then since ζ^a, ζ^b , and ζ^c each have prime power order, this would contradict (3.1). Thus k is a power of a prime y , and so, by (3.1), at least two of a, b, c are relatively prime to k . Assume that

$$\gcd(c, k) = 1. \quad (3.6)$$

(From this point on, we may no longer appeal to symmetry in a, b, c .) For any integer $u \not\equiv 0 \pmod{k}$,

$$N(\lambda_u) = y, \quad (3.7)$$

where N denotes the norm from $\mathbb{Q}(\zeta)$ to \mathbb{Q} . By (3.6), $\lambda = 1 - \zeta$ and $\lambda_c = 1 - \zeta^c$ are associates.

Since $\zeta \equiv 1 \pmod{\lambda}$, (3.3) yields

$$\begin{aligned} \frac{F}{\lambda_a \lambda_b} &= - \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} \frac{\lambda_a^{\text{ind}(\alpha)}}{\lambda_a} \frac{\lambda_b^{\text{ind}(-1-\alpha)}}{\lambda_b} \\ &\equiv - \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} \text{ind}(\alpha)(\text{ind}(-1-\alpha)) \pmod{\lambda}. \end{aligned} \quad (3.8)$$

Whether q is odd or even, it is easily seen that $\text{ind}(-1-\alpha) \equiv \text{ind}(1+\alpha) \pmod{\lambda}$.

Thus,

$$\frac{F}{\lambda_a \lambda_b} \equiv - \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} (\text{ind } \alpha)(\text{ind}(1 + \alpha)) \equiv -L \pmod{\lambda},$$

where L is defined in (2.4). If $k > 4$, it follows from (2.10) that $\lambda \mid L$, and so

$$F \equiv 0 \pmod{\lambda_a \lambda_b \lambda_c}, \quad \text{if } k > 4. \quad (3.9)$$

Also, by (2.10),

$$F \equiv -f \lambda_a \lambda_b \pmod{\lambda_a \lambda_b \lambda_c}, \quad \text{if } k = 3 \text{ or } 4. \quad (3.10)$$

First suppose that $k = 3$. Then (3.10) is equivalent to

$$F \equiv 3f(-1 \pm i\sqrt{3})/2 \equiv (1 - q)/2 \pmod{3\sqrt{3}}.$$

Then since $\chi(-1) = 1$, (3.2) and (3.4) yield

$$J(a, b) = F + E \equiv (1 - q)/2 + q \equiv 2 - q \pmod{3\sqrt{3}}.$$

This completes the proof of Theorem 1 when $k = 3$.

Next suppose that $k = 4$. Then (3.10) is equivalent to

$$F \equiv 2f(1 \pm i) \equiv (1 + i)(q - 1)/2 \pmod{4}.$$

Since $\chi(-1) = (-1)^f$, (3.4) yields

$$E \equiv \begin{cases} q \equiv 1 \pmod{4}, & \text{if } 2 \mid f \\ q - 2 \equiv -1 \pmod{4}, & \text{if } 2 \nmid f. \end{cases}$$

Thus

$$J(a, b) = F + E \equiv 1 + i(q - 1)/2 \pmod{4},$$

which completes the proof when $k = 4$.

Finally, suppose that $k > 4$. Then by (3.9) and (3.4),

$$J(a, b) = F + E \equiv q - 2 + \chi^a(-1) + \chi^b(-1) \pmod{\lambda_a \lambda_b \lambda_c}.$$

Since k is a prime power > 4 , $\lambda_a \lambda_b \lambda_c$ divides k . Thus, to prove (1.6), it remains to prove that

$$q - 2 + \chi(-1)^a + \chi(-1)^b \equiv \chi(-1) \pmod{k}. \quad (3.11)$$

If $\chi(-1) = 1$, then (3.11) is clear. If $\chi(-1) = -1$ (so that $2 \mid k$), then (3.11) again follows if a and b have opposite parity. There are no other possibilities, since if $\chi(-1) = -1$ with a and b both odd, this would contradict (3.6). ■

4. PROOF OF THEOREM 2

It suffices to prove the congruence (1.7) modulo $\lambda_a \lambda_b \lambda_2$, because c is odd and λ_2 is an associate of λ^2 . Since a and b have opposite parity, the expression E in (3.4) satisfies $E \equiv \chi(-1) \pmod{k}$. Then since $\lambda_a \lambda_b \lambda_2$ divides k (because $8 \mid k$), it follows from (3.2)–(3.4) that

$$R := \frac{J(a, b) - \chi(-1)}{\lambda_a \lambda_b} \equiv \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} \frac{\lambda_a^{\text{ind}(\alpha)}}{\lambda_a} \frac{\lambda_b^{\text{ind}(-1-\alpha)}}{\lambda_b} \pmod{\lambda_2}. \quad (4.1)$$

Since b is even and $\zeta^2 \equiv 1 \equiv -1 \pmod{\lambda_2}$,

$$\frac{\lambda_b^{\text{ind}(-1-\alpha)}}{\lambda_b} \equiv \text{ind}(-1-\alpha) \equiv \text{ind}(1+\alpha) \pmod{\lambda_2}. \quad (4.2)$$

When $\text{ind}(\alpha)$ is even,

$$\begin{aligned} \frac{\lambda_a^{\text{ind}(\alpha)}}{\lambda_a} &\equiv (1-\zeta) + \zeta^2(1-\zeta) + \zeta^4(1-\zeta) + \zeta^{(\text{ind} \alpha)-2}(1-\zeta) \\ &\equiv (1-\zeta)(\text{ind} \alpha)/2 \pmod{\lambda_2}, \end{aligned} \quad (4.3)$$

and when $\text{ind}(\alpha)$ is odd,

$$\frac{\lambda_a^{\text{ind}(\alpha)}}{\lambda_a} \equiv 1 + (1-\zeta)(-1 + \text{ind} \alpha)/2 \pmod{\lambda_2}. \quad (4.4)$$

By (4.1)–(4.4),

$$\begin{aligned} R &\equiv \frac{(1-\zeta)}{2} \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} (\text{ind} \alpha)(\text{ind}(1+\alpha)) \\ &\quad + \frac{(1+\zeta)}{2} \sum_{\substack{\alpha \in F_q^* \\ \text{ind}(\alpha) \text{ odd}}} \text{ind}(1+\alpha) \pmod{\lambda_2}. \end{aligned} \quad (4.5)$$

The first term on the right side of (4.5) is

$$(1-\zeta) L/2 \equiv (1-\zeta) kf/8 \pmod{\lambda_2},$$

by (2.6). The second term is

$$\frac{(1+\zeta)}{2} \sum_{\substack{s, t \pmod{k} \\ s \text{ odd}}} t(s, t)_k \equiv \frac{(1+\zeta)}{2} (\text{ind } 2) \equiv (1-\zeta)(\text{ind } 2)/2 \pmod{\lambda_2},$$

by Proposition 8. Thus (4.5) becomes

$$R \equiv (1-\zeta)(kf/8 + (\text{ind } 2)/2) \pmod{\lambda_2},$$

and so (1.7) follows upon multiplying by $\lambda_a \lambda_b$. ■

5. PROOF OF THEOREM 3

Let $k \geq 4$ be even. By (1.1),

$$J(a, d) - J(b, d) = \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} (1 - \chi^d(-1 - \alpha))(1 - \chi^{b-a}(\alpha)) \chi^a(\alpha),$$

since $\chi^a(-1) = \chi^b(-1)$. Thus, since $2 \mid d$, $2 \mid (b-a)$, $2 \nmid a$, and $\zeta^2 \equiv 1 \pmod{\lambda_2}$,

$$T := \frac{J(a, d) - J(b, d)}{\lambda_d \lambda_{b-a}} \equiv \sum_{\substack{\alpha \in F_q \\ \alpha \neq 0, -1}} (\text{ind}(-1 - \alpha))(\text{ind } \alpha) \zeta^{\text{ind}(\alpha)} \pmod{\lambda_2}.$$

Since $\text{ind}(-1 - \alpha) \equiv \text{ind}(1 + \alpha)$ modulo $k/2$ and hence modulo λ_2 ,

$$T \equiv \sum_{s, t \pmod{k}} st(s, t)_k \zeta^s \pmod{\lambda_2}.$$

Therefore, in the notation of (2.11) and (2.4),

$$T \equiv N + \zeta(L - N) \pmod{\lambda_2}. \quad (5.1)$$

Suppose that $k \geq 4$ is a power of 2. By (2.12) and (2.6), N and L are both even, except that L is odd in the case when $k = 4$, $2 \nmid f$. Thus, if $k = 4$, then $T \equiv fi$ modulo $\lambda_2 = 2$, so that

$$J(1, 2) \equiv J(3, 2) + 4if \pmod{8}, \quad (5.2)$$

while if k is a power of 2 exceeding 4,

$$J(a, d) \equiv J(b, d) \pmod{\lambda_d \lambda_{b-a} \lambda_2}. \quad (5.3)$$

Since λ_2 is a unit unless $k/2$ is a prime power, it remains to consider the case where $k/2$ is a power of an odd prime y . By (2.12), N is divisible by

y (and hence by λ_2), unless $k=6$, in which case $N \equiv f \pmod{3}$. By (2.6), L is divisible by y , unless $k=6$, in which case $L \equiv -f \pmod{3}$. Thus by (5.1), $T \equiv 0 \pmod{\lambda_2}$, since even in the case $k=6$, we have

$$T \equiv f + \zeta(-f - f) \equiv f(1 + \zeta) = f(1 - \zeta^4) \equiv 0 \pmod{\lambda_2}.$$

Thus (5.3) holds for all even $k > 4$. ■

6. PROOF OF COROLLARY 4

By a simple case of the Davenport–Hasse multiplication theorem [3, Theorem 2.1.4],

$$\chi(-4^d) J(d, d) = J(k/2, d).$$

Thus, by Theorem 3,

$$\chi(-4^d) J(d, d) \equiv J(a, d) \pmod{\lambda_2^3}. \quad (6.1)$$

By Theorem 1 with $k/\gcd(k, d)$ in place of k , we have

$$J(d, d) \equiv \begin{cases} 1 \pmod{\lambda_2^3}, & \text{if } k \nmid 3d, \\ 2 - q \pmod{\lambda_2^3}, & \text{if } k \mid 3d. \end{cases} \quad (6.2)$$

The result (1.10) now follows from (6.1) and (6.2). ■

REFERENCES

1. H. Abo, N. Sasakura, and T. Terasoma, Quadratic residue graph and Shioda elliptic modular surface $S(4)$, *Tokyo J. Math.* **19** (1996), 263–288.
2. V. V. Acharya and S. A. Katre, Cyclotomic numbers of order $2l$, l an odd prime, *Acta Arith.* **69** (1995), 51–74.
3. B. C. Berndt, R. J. Evans, and K. S. Williams, “Gauss and Jacobi Sums,” Wiley Interscience, New York, 1998.
4. R. J. Evans, The 2^r -th power character of 2, *J. reine angew. Math.* **315** (1980), 174–189.
5. F. Gouvêa and N. Yui, “Arithmetic of Diagonal Hypersurfaces over Finite Fields,” Cambridge Univ. Press, Cambridge, 1995.
6. Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, *Annals of Math.* **123** (1986), 43–106.
7. K. Iwasawa, “A note on Jacobi sums,” *Symposia Math.*, Vol. 15, pp. 447–459, Academic Press, London, 1975.
8. H. Miki, On the l -adic expansion of certain Gauss sums and its applications, in “Galois Representations and Arithmetic Algebraic Geometry” (Y. Ihara, Ed.), *Advanced Studies in Pure Mathematics*, Vol. 12, pp. 87–118, North-Holland, Amsterdam, 1987.